

(19)



JAPANESE PATENT OFFICE

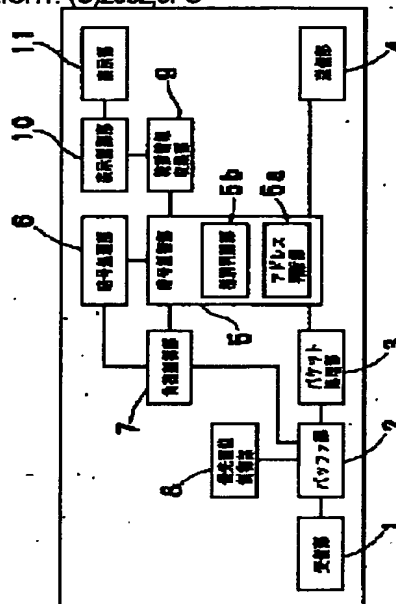
PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002064482 A**(43) Date of publication of application: **28.02.02**(51) Int. Cl. **H04L 9/14**(21) Application number: **2000252787**(22) Date of filing: **23.08.00**(71) Applicant: **MATSUSHITA ELECTRIC WORKS LTD**(72) Inventor: **MIURA TOSHIBUMI****(54) ENCRYPTION APPARATUS****(57) Abstract**

PROBLEM TO BE SOLVED: To provide an encryption apparatus for reducing the amount of scrap of received data and preventing the capacity of the whole network from being reduced.

SOLUTION: The encryption apparatus comprises a receiving section 1 for receiving data from the outside, a transmitting section 2 for transmitting the data to the outside, an encryption control section 5 for making a judgment whether the encrypting of the data received from the receiving section is necessary or not based on the address from which the data is transmitted or the address to which the data is transmitted, an encryption section 6 for encrypting the data, which the encryption section 5 judges to be encrypted, by the use of one encryption mode of a plurality of encryption modes and for outputting the encrypted data to the transmitting section 2, and a load control section 7 for monitoring the encrypting load of the encryption section 6 and changing the encryption mode of the encryption section 6 according to the encrypting load.

COPYRIGHT: (C)2002 JPO



(11)特許出願公開番号
特開2002-64482
(P2002-64482A)

【特許請求の範囲】

【請求項 1】 外部からデータを受信する受信部と、外部にデータを送信する送信部と、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断する暗号制御部と、該暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理し処理結果のデータを送信部に出力する暗号処理部と、を備えた暗号処理装置において、

暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更する負荷制御部を備えたことを特徴とする暗号処理装置。

【請求項 2】 前記負荷制御部は、暗号処理部における暗号処理の負荷が高負荷である場合に、暗号処理部の暗号方式をより負荷の軽い暗号方式に変更することを特徴とする請求項 1 記載の暗号処理装置。

【請求項 3】 前記暗号制御部に、データの種別を判別し、該種別によって暗号処理の要否を判断する種別判断部を設け、該種別判断部は暗号処理を要すると判断したデータを暗号処理部に出力することを特徴とする請求項 1 又は請求項 2 記載の暗号処理装置。

【請求項 4】 前記暗号処理部は、前記種別判断部の判別しする種別に応じた暗号方式で暗号処理することを特徴とする請求項 3 記載の暗号処理装置。

【請求項 5】 前記受信部と暗号制御部との間に、受信したデータを一時的に蓄積記憶するバッファ部と、該バッファ部内に蓄積記憶されているデータに優先順位を付する優先順位制御部とを設け、暗号制御部は、前記優先順位の高いデータから暗号処理の要否を判断することを特徴とする請求項 1 乃至請求項 4 のいずれかに記載の暗号処理装置。

【請求項 6】 前記暗号処理部の暗号処理に用いる暗号方式を表示する表示部を設けたことを特徴とする請求項 1 乃至請求項 5 記載の暗号処理装置。

【請求項 7】 外部からデータを受信するステップと、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断するステップと、該暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理するステップと、処理結果のデータを送信するステップと、を備えた暗号処理方法において、

暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するステップを備えたことを特徴とする暗号処理方法。

【請求項 8】 前記負荷を監視して暗号方式を変更するステップは、暗号処理の負荷が高負荷である場合に、暗号方式をより負荷の軽い暗号方式に変更することを特徴とする請求項 7 記載の暗号処理方法。

【請求項 9】 前記暗号処理の要否を判断するステップ

に、データの種別を判別し、該種別によって暗号処理の要否を判断するステップを設けたことを特徴とする請求項 7 又は請求項 8 記載の暗号処理方法。

【請求項 10】 前記暗号処理するステップは、前記判別した種別に応じた暗号方式で暗号処理することを特徴とする請求項 9 記載の暗号処理方法。

【請求項 11】 データを受信するステップの後に、受信したデータを一時的に蓄積記憶するステップと、該蓄積記憶されているデータに優先順位を付するステップとを設け、前記暗号処理の要否を判断するステップは、前記優先順位の高いデータから暗号処理の要否を判断することを特徴とする請求項 7 乃至請求項 10 のいずれかに記載の暗号処理方法。

【請求項 12】 前記請求項 6 乃至請求項 11 のいずれかに記載の暗号処理方法を実行するためのプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一方側から受信したデータを暗号処理して他方側へ送信する暗号処理装置に関する。

【0002】

【従来の技術】 近年、データ通信のセキュリティを目的として、コンピュータ端末近傍に暗号処理装置を配して、当該コンピュータ端末から送信されるデータには暗号化処理を施して暗号データを送信し、コンピュータ端末側に受信される暗号データには復号化処理を施して通常のデータとして受信する場合がある。このような場合に用いられる暗号処理装置にあっては、データの送信元アドレスや送信先アドレスなどによって暗号処理をデータに施すか否かを判断して、必要なものを暗号処理して送受信するということが行われている。

【0003】

【発明が解決しようとする課題】 しかしながら、従来の暗号処理装置にあっては、暗号処理に複雑な計算を要するため暗号処理の負荷が大きくなり、次々と受信するデータの処理が間に合わない場合があった。このように先に受信されたデータの暗号処理が終わる前に次のデータが受信された場合、後続のデータは破棄され、データの送信元は再度ネットワーク上にデータを送信しなければならなかった。また、これに対処すべくバッファを設け、該バッファにデータを蓄積して順次処理するものもあるが、次々にデータを受信した場合には処理が間に合わないバッファが溢れてしまい、溢れたデータは破棄され、再度データの送信が行われることとなる。その結果、暗号処理装置を一つのノードとするネットワーク全体の性能を低減させる恐れがあるという問題点があった。

【0004】 本発明は、上記問題点を改善するために成されたもので、その目的とするところは、受信するデー

タの破棄を低減し、ネットワーク全体の性能の低減を防止する暗号処理装置、暗号処理方法及びその方法を実行するプログラムを記録した記録媒体を提供することにある。

【0005】

【課題を解決するための手段】上記の問題を解決するために、本発明の暗号処理装置にあっては、外部からデータを受信する受信部と、外部にデータを送信する送信部と、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断する暗号制御部と、該暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理し処理結果のデータを送信部に出力する暗号処理部と、を備えた暗号処理装置において、暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更する負荷制御部を備えたことを特徴とするものである。

【0006】前記負荷制御部は、暗号処理部における暗号処理の負荷が高負荷である場合に、暗号処理部の暗号方式をより負荷の軽い暗号方式に変更するものであることが好ましい。ここで、高負荷とは、これ以上そのままの処理を継続すると、送信するデータよりも受信するデータが多くなって、全てのデータを処理することができず、受信するデータの一部又は全部を破棄する恐れのあるような場合をいう。

【0007】また、暗号制御部に、データの種別を判別し、該種別によって暗号処理の要否を判断する種別判断部を設け、該種別判断部は暗号処理を要すると判断したデータを暗号処理部に出力するようにしてもよい。種別とは、データが適用されるアプリケーションソフトウェアや、データのタイプなど、データ自体の特徴を表す属性をいう。そして、この場合には、種別判断部は、種別に応じた暗号方式で暗号処理することを暗号処理部に指示することがより好ましい。

【0008】一方、前記受信部と暗号制御部との間に、受信したデータを一時的に蓄積記憶するバッファ部と、該バッファ部内に蓄積記憶されているデータに優先順位を付する優先順位制御部とを設け、暗号制御部は、前記優先順位の高いデータから暗号処理の要否を判断するものであってもよい。

【0009】更に、暗号処理部の暗号処理に用いる暗号方式を表示する表示部を設けるようにしてもよい。また、表示部は暗号方式以外の暗号処理に関する情報を表示するものであってもよい。

【0010】また、本発明の暗号処理方法にあっては、暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するステップを備えたことを特徴とするものである。また、負荷を制御し暗号方式を変更するステップは、暗号処理の負荷が高負荷である場合に、暗号方式をより負荷の軽い暗号方式に変更することを特

徴とするものが好ましい。

【0011】記暗号処理の要否を判断するステップに、データの種別を判別し、該種別によって暗号処理の要否を判断するステップを設けることも好ましく、この場合、暗号処理するステップは、前記判別した種別に応じた暗号方式で暗号処理するようにすればより好ましい。

【0012】一方、データを受信するステップの後に、受信したデータを一時的に蓄積記憶するステップと、該蓄積記憶されているデータに優先順位を付するステップとを設け、暗号処理の要否を判断するステップは、前記優先順位の高いデータから暗号処理の要否を判断するものであってもよい。

【0013】また、本発明の記録媒体にあっては、上記の暗号処理方法を実行するためのプログラムを記録したことを特徴とするものである。

【0014】

【発明の実施の形態】本発明にかかる暗号処理装置の第一実施の形態を図1乃至図5に基づいて説明する。図1は本発明の暗号処理装置の一構成例を示すブロック図であり、図2は暗号処理装置の外観を示す斜視図である。図3は本発明の暗号処理装置の全体の動作を説明するフローチャートである。図4は本発明の暗号処理装置の暗号方式の変更動作の他の例を説明するフローチャートである。

【0015】図1において、暗号処理装置は、受信部1、バッファ部2、パケット処理部3、送信部4、暗号制御部5、暗号処理部6、負荷制御部7、優先順位制御部8、統計情報収集部9、表示制御部10、表示部11を備えて構成されており、特定送信元アドレスからのデータ又は特定宛先アドレスへのデータについて通過させるとともに、更にその中で特定の送信元アドレスからのデータ又は特定宛先アドレスへのデータについてはデータを暗号化して送信させるものである。従って、データには暗号処理装置を通過できないもの、暗号処理装置をそのまま暗号化されずに通過するもの、及び暗号処理装置にて暗号化されて通過するもの、の3種類がある。

【0016】受信部1は、コネクタを有しており該コネクタに接続された信号線を介して外部からのデータを受信するものである。受信されるデータは、暗号化処理がなされておらずそのまま内容の把握が可能な平文データであり、例えばパケットの形式をとっている。受信部1は、データを受信すると、該データをバッファ部2に出力する。

【0017】バッファ部2は、受信したデータを一時的に蓄積記憶するものであり、読み書き可能なメモリで構成されている。バッファ部2は、データを受け取ると、待ち行列の最後尾にデータを格納する。バッファ部2を設けることにより、前のデータの暗号処理が終了するまでに次のデータを受信しても、該次のデータを蓄積記憶できるため、データの破棄を防止することができる。

【0018】パケット処理部3は、バッファ部2の待ち行列の先頭からデータを取り出して、暗号処理装置を通して良いか否かを判断するものである。パケット処理部3は、バッファ部2の暗号処理装置の通過を許可する特定の送信元アドレスからのデータ又は特定宛先アドレスへのデータについては暗号制御部5に出力し、暗号処理装置の通過を許可しない他のデータについてはデータを破棄する。なお、データの送信元アドレス又は宛先アドレスと、通過の要否との関係は、別途設定テーブルを設けておいて、パケット処理部3は該テーブルを参照して判断するようになしてある。

【0019】暗号制御部5は、暗号処理装置を通してデータについて、暗号処理を行うか否かを判断するものであり、アドレス判断部5aと、種別判断部5bとを備えている。

【0020】アドレス判断部5aは、データの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断するものであり、暗号処理を必要としないデータについてはそのまま送信部4に出力し、暗号処理が必要なデータについては種別判断部5bに出力する。なお、データの送信元アドレス又は宛先アドレスと、暗号処理の要否との関係は、別途設定テーブルを設けておいて、アドレス判断部5aは該テーブルを参照して判断するようになしてある。

【0021】種別判断部5bは、データの種別を判別し、該種別によって暗号処理の要否を判断するものである。種別とは、特定のワードプロセッサや特定の画像処理ソフトウェア等のようにデータが対応するアプリケーションソフトウェアの種類であってもよいし、テキストデータ、イメージデータなどのデータのタイプであってもよい。本実施の形態では、データが対応するアプリケーションソフトウェアの種類を種別として用いている。種別判断部5bは、データの種別に基づいて暗号処理を必要としないと判断したデータについてはそのまま送信部4に出力し、データの種別に基づいて暗号処理が必要と判断したデータについては暗号処理部6に出力する。その際、種別判断部5bは、種別に応じた暗号方式で暗号処理することを暗号処理部に指示するようになしてある。具体的には、種別判断部5bは、例えばアプリケーションソフトウェアPに対応するデータについては、暗号方式Xにて暗号処理を行うように指示し、アプリケーションソフトウェアQに対応するデータについては、暗号方式Yにて暗号処理を行うように指示する。なお、種別と、暗号処理の要否及び暗号方式との関係は、別途設定テーブルを設けておいて、種別判断部5bは該テーブルを参照して判断するようになしてある。

【0022】種別判断部5bにより、データの種別により暗号処理の要否判断を行うことにより、データの種別によっては暗号処理が不要となる場合に、該不要な暗号処理を行うことがなく、よって暗号処理動作の負荷を軽

減することができる。つまり、アドレス判断部5aにて暗号処理を要すると一律に判断されたデータの中でも、データの種別によっては暗号処理をする必要のないものが存在する場合があります、これらデータの暗号処理を省くことにより暗号処理動作の負荷を軽減することが可能となる。また、種別判断部5bは、種別に応じた暗号方式で暗号処理することを暗号処理部に指示するため、種別に応じた暗号強度を選択することが可能となり、一律の暗号強度とする場合に比べて暗号処理の効率を高めることが可能となる。

【0023】暗号処理部6は、例えばシングルDES方式やトリプルDES方式等の複数の暗号方式による暗号処理が可能であって、暗号制御部5から受け取ったデータを、種別判断部5bの指定する暗号方式により暗号化するものである。但し、暗号処理部6は次に説明する負荷制御部7からも暗号方式を指定される場合があります、負荷制御部7から指定があった場合には、その指定に優先して従うようになしてある。暗号処理部6は、暗号処理されたデータを暗号制御部5を介して送信部4に出力する。

【0024】負荷制御部7は、暗号処理部6の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部6の暗号方式を変更するものである。負荷制御部7は、暗号処理動作の負荷が所定の負荷閾値A以上の場合である高負荷の場合には、暗号方式をより負荷の軽い他の暗号方式に変更するよう暗号処理部6に指示をする。負荷閾値は、暗号処理部6にかかる負荷を表す値であれば良いが、本実施の形態ではバッファ部2に蓄積される未処理のデータ個数としている。

【0025】具体的には、負荷制御部7は、バッファ部2の待ち行列に入っているデータの個数を検出して、バッファ部2の待ち行列からデータが溢れそうな程度にデータが蓄積記憶されている場合に、暗号処理動作が高負荷であると判断する。例えば、負荷制御部7は、バッファ部2の待ち行列の8割にデータが記憶された場合に、負荷閾値A以上であり高負荷と判断する。そして、負荷制御部7は、暗号処理動作が高負荷であると判断した場合には、暗号処理部6の暗号方式をより負荷の軽い暗号方式に変更するよう、暗号処理部6に指示を出す。例えば、暗号制御部7は、暗号処理部6が暗号方式Yで暗号処理を行おうとしている場合に、より負荷の軽い暗号方式Xへの変更を指示する。

【0026】優先順位制御部8は、バッファ部2内に蓄積記憶されているデータに優先順位を付するものであり、優先順位の高いデータが待ち行列の先頭となるようにデータを制御するものである。この場合、優先順位制御部8は、待ち行列に入るデータを記憶し直してメモリの中で物理的にデータが優先順位の順番に並ぶようにしてもよいし、データに優先順位を示すインデックスを別途設けておいて、論理的に優先順位の順番にならぶよう

にして、パケット処理部 3 がインデックスに示された優先順位順にデータを取り出すようにしてもよい。優先順位制御部 8 は、データのプロトコル、対応アプリケーションソフトウェア、ファイルタイプ、宛先アドレス、送信元アドレス等に基づいて優先順位を決定する。

【0027】統計情報収集部 9 は、暗号処理部 6 の処理する暗号方式について、各暗号方式の使用回数、暗号方式の変更回数等の各種の統計情報、及び現在処理中の暗号方式を収集するものである。

【0028】表示制御部 10 は、統計情報収集部 9 の収集した統計情報及び現在処理中の暗号方式を表示部 11 に出力するものである。具体的には、表示制御部 10 は、図 2 に示すように、統計情報を表示部 11 の液晶表示部 11a に出力して文字や図形情報として視覚化し、現在処理中の暗号方式については表示部 11 の LED 表示部 11b に出力する。LED 表示部 11b は複数の LED を備えており、点灯パターンにより暗号方式を示すようになしてある。

【0029】次に以上のようにして構成した暗号処理装置の動作を図 3 を用いて説明する。

【0030】まず、受信部 1 がデータをパケット形式で受信して（ステップ S101）、該受信データをバッファ部 2 に蓄積記憶する。その際に、優先順位制御部 8 が該蓄積記憶されているデータに優先順位を付与する（ステップ S101）。そして、パケット処理部 3 が、バッファ部 2 の待ち行列の中から優先順位の最も高いデータを取り出して、送信元アドレス、宛先アドレスに基づいて、データを通過させてよいか否かを判断する（ステップ S102）。

【0031】パケット処理部 3 は、データを通過させてもよいと判断した場合には、該データを暗号制御部 5 に出力する。暗号制御部 5 では、まずアドレス判断部 5a がデータの送信元アドレス、宛先アドレスから暗号処理の要否を判断し（ステップ S103）、暗号処理不要と判断されたデータはそのまま送信される（ステップ S112）。一方、暗号処理が必要と判断されたデータは、種別判断部 5b に出力され、更にデータの種別に基づいて、暗号処理の要否が判断される（ステップ S104）。具体的には、本実施の形態では、データに対応するアプリケーションソフトウェアに基づいて暗号処理の要否を判断するようにしてある。そして、暗号処理不要と判断されたデータはそのまま送信され（ステップ S112）、暗号処理が必要と判断されたデータは暗号処理部 6 に出力されるとともに、種別判断部 5b は暗号方式を指定して暗号処理部 6 に指示を行う（ステップ S105～S107）。

【0032】次に負荷制御部 7 は、現在の暗号処理部 6 における暗号処理の負荷を監視し、現在の暗号方式を確認した上で（ステップ S108）、暗号方式として処理負荷の高い暗号方式 Y が指定されており、暗号処理動作

の負荷が所定の負荷閾値 A 以上の場合である高負荷の場合には（ステップ S109）、暗号方式 Y をより負荷の軽い暗号方式 X に変更するよう暗号処理部 6 に指示をし（ステップ S110）、暗号処理動作の負荷が所定の負荷閾値 A 未満の場合であるには暗号方式の変更は行わない。また、暗号方式として負荷の軽い暗号方式 X が指定されている場合にも、暗号方式を変更することなく処理を続行する（ステップ S108）。

【0033】以上のようにして指定された暗号方式に基づいて、暗号処理部 6 はデータを暗号化し（ステップ S111）、該暗号化したデータを暗号制御部 5 を介して送信部 4 に出力する。送信部 4 は該データを外部に送信し（ステップ S112）、一連の動作が完了する。該動作は繰り返し行われる。但し、ステップ S102～ステップ S112 までの一連の流れは連続して 1 ステップづつ行われるが、データの受信処理（ステップ S101）は上記一連の流れとは別個に行われる。

【0034】なお、上記説明では、暗号処理動作の負荷が軽い場合には特に暗号方式を変更することはしていないが、図 4 に示すように、より負荷の高い暗号方式に変更する（ステップ S113、S114）ようにしてもよい。この場合、暗号処理装置の負荷が軽い場合にはより強度の暗号化を行ったデータを送信することができるという利点がある。

【0035】以上のようにして構成した暗号処理装置及び暗号処理方法にあつては、負荷が高くなりバッファ部 2 からデータが溢れそうになった場合に、暗号処理部 6 での暗号方式を負荷の軽いものに変更するので、データ溢れを防止して、データが破棄されることを防ぐことができ、ひいては暗号処理装置を一つのノードとするネットワーク全体の性能の低下を防止することができる。

【0036】なお、本発明の暗号処理装置は、上述したもののみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【0037】

【発明の効果】本発明の暗号処理装置は上述のように構成してあるから、請求項 1 記載の発明にあつては、負荷制御部が、暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するので、負荷状況に対応した暗号方式を用いることができるという効果を奏する。

【0038】請求項 2 記載の発明にあつては、負荷制御部は、暗号処理部における暗号処理の負荷が高負荷である場合に、暗号処理部の暗号方式をより負荷の軽い暗号方式に変更するので、暗号処理動作の過負荷によるデータの破棄を防止し、ネットワーク全体の性能の低下を防止することができるという効果を奏する。

【0039】請求項 3 記載の発明にあつては、暗号制御部に、データの種別を判別し、該種別によって暗号処理

の要否を判断する種別判断部を設け、該種別判断部は暗号処理を要すると判断したデータを暗号処理部に出力するので、データの種別によっては暗号処理が不要となる場合に、該不要な暗号処理を行うことがなく、よって暗号処理動作の負荷を軽減することができるという効果を奏する。

【0040】請求項4記載の発明にあつては、暗号処理部が、種別判断部の判別する種別に応じた暗号方式で暗号処理するので、データの種別毎に暗号強度を適宜設定でき、効率的に暗号処理をすることにより、暗号処理動作の負荷を軽減することができるという効果を奏する。

【0041】請求項5記載の発明にあつては、優先順位制御部が、バッファ部内に蓄積記憶されているデータに優先順位を付け、暗号制御部は、優先順位の高いデータから暗号処理の要否を判断するので、優先順位の高いデータをより素早く処理して送信することができるという効果を奏する。

【0042】請求項6記載の発明にあつては、表示部が暗号処理部の暗号処理に用いる暗号方式を表示するので、使用者は現在の暗号方式を目視確認することができ、暗号処理装置の誤動作の確認をすることが容易になるという効果を奏する。

【0043】請求項7記載の発明にあつては、暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するステップを備えたので、負荷状況に対応した暗号方式を用いることができるという効果を奏する。

【0044】請求項8記載の発明にあつては、負荷を制御し暗号方式を変更するステップは、暗号処理の負荷が高負荷である場合に、暗号方式をより負荷の軽い暗号方式に変更するので、暗号処理動作の過負荷によるデータの破棄を防止し、ネットワーク全体の性能の低下を防止することができるという効果を奏する。

【0045】請求項9記載の発明にあつては、暗号処理の要否を判断するステップに、データの種別を判別し、該種別によって暗号処理の要否を判断するステップを設けたので、データの種別によっては暗号処理が不要となる場合に、該不要な暗号処理を行うことがなく、よって

暗号処理動作の負荷を軽減することができるという効果を奏する。

【0046】請求項10記載の発明にあつては、暗号処理するステップは、判別した種別に応じた暗号方式で暗号処理するので、データの種別毎に暗号強度を適宜設定でき、効率的に暗号処理をすることにより、暗号処理動作の負荷を軽減することができるという効果を奏する。

【0047】請求項11記載の発明にあつては、データを受信するステップの後に、受信したデータを一時的に蓄積記憶するステップと、該蓄積記憶されているデータに優先順位を付するステップとを設け、暗号処理の要否を判断するステップは、前記優先順位の高いデータから暗号処理の要否を判断するので、優先順位の高いデータをより素早く処理して送信することができるという効果を奏する。

【0048】請求項12記載の発明にあつては、記録媒体をコンピュータ等に読み込み実行させることにより、請求項7乃至請求項11のいずれかに記載の発明の効果を奏する。

20 【図面の簡単な説明】...

【図1】本発明の暗号処理装置の構成の一例を示すブロック図である。

【図2】本発明の暗号処理装置の外観を示す斜視図である。

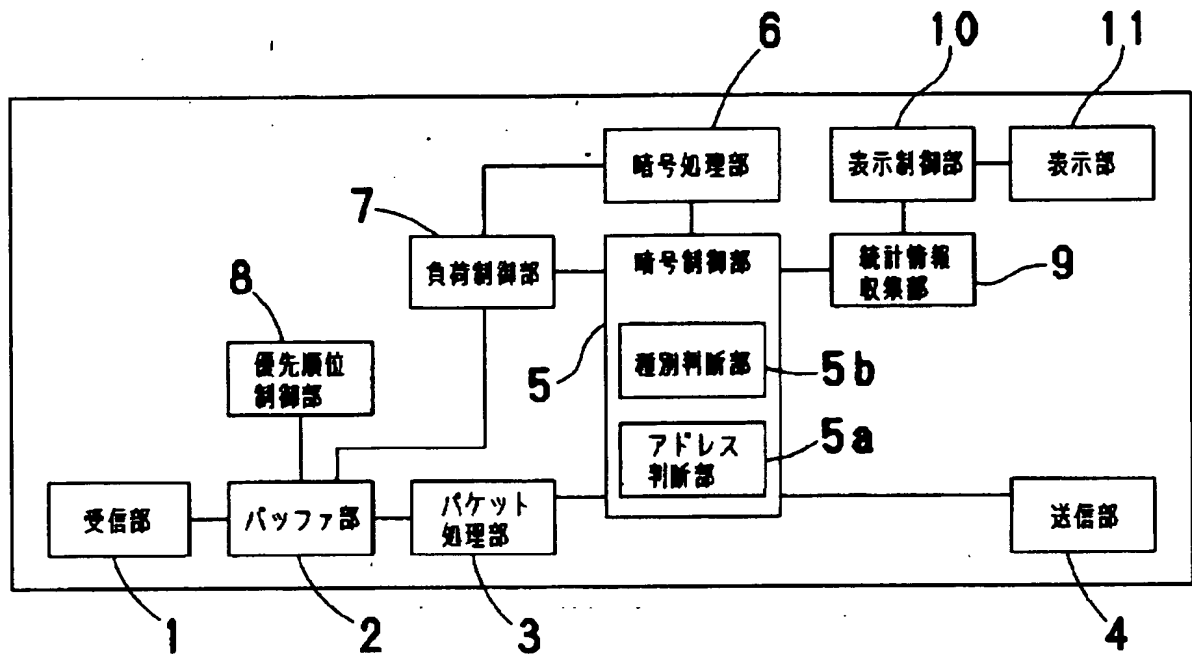
【図3】本発明の暗号処理方法の一例を示すフローチャートである。

【図4】本発明の暗号処理方法の他の例を示すフローチャートである。

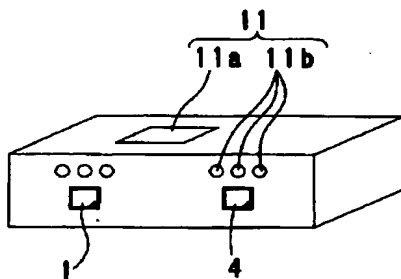
【符号の説明】

- 30 1 受信部
2 バッファ部
4 送信部
5 暗号制御部
5b 種別判断部
6 暗号処理部
7 負荷制御部
8 優先順位制御部
11 表示部

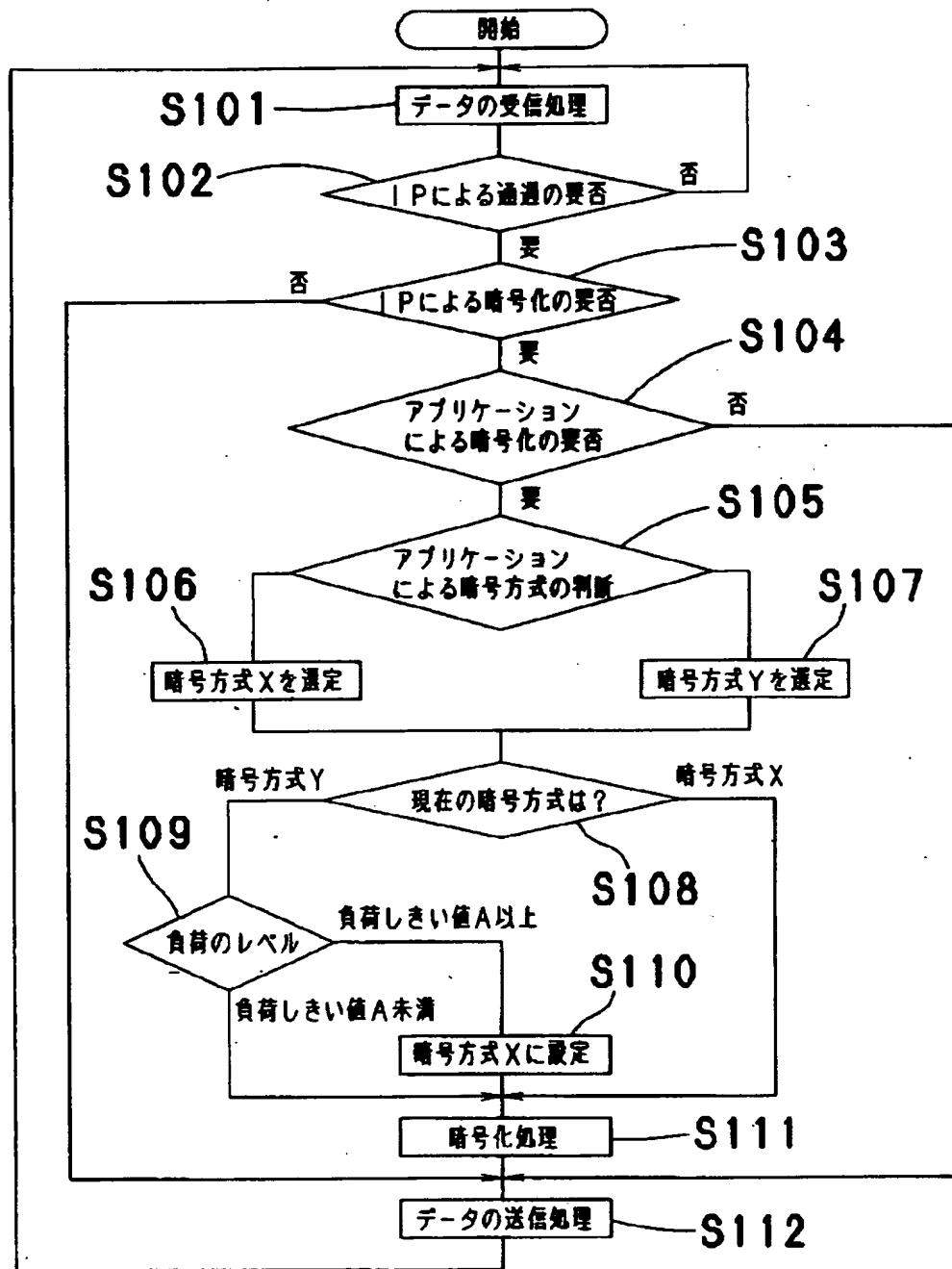
【図1】



【図2】



【図3】



【図4】

